DIJEMSS: Dinasti International Journal of Education Management and Social Science
E-ISSN: 2686-6331
P-ISSN: 2686-6358
https://dinastipub.org/DIJEMSS dinasti.info@gmail.com +62 811 7404 455
DOI: https://doi.org/10.38035/dijemss.v7i4

The Factors Influencing Maritime Cyber Security Resiliency in Indonesia : The Mediating Role of Cyber Security Awareness

Arizal Hendriawan[1], Idris Gautama[2], Denny Siahaan[3], Kurniawan[4]
[1]Institute of Transportation and Logistics Trisakti, Jakarta, Indonesia, arizal1975@gmail.com
[2]Bina Nusantara University, Jakarta, Indonesia, igautama@binus.edu
[3]Institute of Transportation and Logistics Trisakti, Jakarta, Indonesia, langasdennysiahaan@gmail.com
[4]Nusa Putra University, Jakarta, Indonesia, kurniawan@nusaputra.ac.id

Corresponding Author: arizal1975@gmail.com[1]

Abstract: Digitalization in maritime operations has increased cyber risks to shipboard systems and navigational safety. This study examines the effects of procedure availability, IT system availability, and monitoring on MCS Resiliency, with MCS Awareness as a mediator and fear of cyber attack as a moderator. A quantitative survey was conducted with 400 Indonesian shipboard officers holding valid Certificates of Endorsement, and data were analyzed using SEM-PLS. The results show that procedures, IT system availability, and monitoring significantly influence both MCS Awareness and MCS Resiliency. MCS Awareness also has a significant positive effect on MCS Resiliency and mediates the relationships between the three antecedent variables and resilience. However, fear of cyber attack does not significantly moderate the relationship between MCS Awareness and MCS Resiliency. These findings highlight that maritime cyber resilience is primarily driven by structured governance, resilient technology, effective monitoring, and awareness-based competence rather than fear-based motivation. The study provides empirical support for a human-centered and system-oriented approach to strengthening maritime cybersecurity.

Keywords: Maritime Cyber Security, Cyber Resilience, Cyber Security Awareness, Procedure Availability, IT System Availability, Monitoring, Seafarers, Shipboard Operations.

INTRODUCTION

The rapid digital transformation of the maritime industry has significantly increased the reliance of ships on information technology (IT) and operational technology (OT) systems, including Electronic Chart Display and Information Systems (ECDIS), Global Positioning Systems (GPS), Automatic Identification Systems (AIS), and network-based communication platforms. While these technologies enhance navigational accuracy, operational efficiency, and connectivity, they simultaneously introduce substantial cyber vulnerabilities that may threaten the safety, reliability, and continuity of maritime operations (Heering et al., 2021 ; Yoo & Park, 2021). High-profile cyber incidents, such as the NotPetya attack on Maersk that caused losses of approximately USD 300 million, demonstrate that cyber threats in the maritime sector are no longer theoretical but constitute real and escalating operational risks (Karas, 2023).

In response to this evolving threat landscape, the concept of Maritime Cyber Security Resiliency (MCS Resiliency) has gained increasing attention. Cyber resiliency refers to the ability to anticipate, withstand, respond to, and recover from cyber incidents while maintaining essential functions (Erstad et al., 2021) . Contemporary cybersecurity literature emphasizes that technical robustness alone is insufficient to achieve resilience; instead, human and organizational dimensions play a decisive role (Afenyo & Caesar, 2023). Within this context, Maritime Cyber Security Awareness (MCS Awareness) is widely recognized as a foundational mechanism that shapes secure behavior and operational readiness against cyber threats.

One of the primary organizational factors influencing MCS Awareness is the presence of clearly defined and consistently implemented procedures. Cybersecurity procedures embedded within safety and operational management systems provide structured guidance on access control, system usage, incident reporting, and emergency response. Such procedures enhance users' understanding of their responsibilities and reduce ambiguity in handling abnormal cyber events (Cook, 2020). Empirical studies indicate that organizations with well-established cybersecurity procedures exhibit higher levels of user awareness and compliance, which in turn strengthen overall cyber preparedness.

Another critical determinant of MCS Awareness is IT System Availability, which refers to the reliability, accessibility, and adequacy of onboard information systems and supporting infrastructure. The availability of secure, well-maintained, and regularly updated IT systems enables seafarers to interact with technology in a controlled and predictable environment, fostering familiarity with security features and system limitations. Research suggests that organizations with robust IT infrastructures tend to demonstrate higher cybersecurity awareness, as users are more frequently exposed to authentication mechanisms, access controls, and system alerts (Waqas et al., 2021). Conversely, outdated or unstable systems increase vulnerability and may undermine users' confidence in cybersecurity measures.

In addition, monitoring plays a vital role in shaping MCS Awareness. Monitoring encompasses continuous system surveillance, log analysis, vulnerability assessments, and anomaly detection aimed at identifying potential cyber threats at an early stage. Effective monitoring not only strengthens technical defenses but also enhances situational awareness among users by providing visibility into security conditions and potential risks (Vaarandi, Tsiopoulos, Visky, & Rehman, 2025). Prior studies demonstrate that monitoring technologies based on correlation and anomaly analysis significantly improve organizations' ability to recognize suspicious activities and promote proactive cybersecurity behavior (Troullinos, 2022).

Collectively, procedures, IT system availability, and monitoring are expected to enhance MCS Awareness, which subsequently contributes to stronger MCS Resiliency. Individuals with higher levels of cybersecurity awareness are more likely to adhere to security policies, exercise caution in system usage, and promptly report incidents, thereby improving an organization's capacity to withstand and recover from cyber disruptions (Netshiunda & Madzvamuse, 2025) This highlights the mediating role of MCS Awareness in translating organizational and technical factors into resilient cybersecurity outcomes.

Furthermore, psychological factors, particularly Fear of Cyber Attack, are increasingly recognized as influential in shaping cybersecurity behavior. Fear reflects individuals' perception of the severity and likelihood of cyber threats and their potential consequences. According to Protection Motivation Theory, heightened threat appraisal combined with perceived response efficacy encourages individuals to adopt protective behaviors. Empirical evidence indicates that fear of cyber attacks can strengthen vigilance, compliance with security procedures, and risk-avoidance behavior (Vrhovec & Mihelič, 2021 ; Raymaker, 2024). Accordingly, fear of cyber attack is expected to moderate the relationship between MCS Awareness and MCS Resiliency by amplifying the impact of awareness on resilient behavior.

Despite growing international attention to maritime cybersecurity, empirical studies that integrate procedures, IT system availability, monitoring, awareness, psychological factors, and resiliency into a single explanatory framework remain limited, particularly in developing maritime nations. Existing research predominantly focuses on technical architectures or regulatory aspects, while the human-centered mechanisms through which organizational and technical factors shape resilience are insufficiently explored. Therefore, this study seeks to address this gap by empirically examining the effects of Procedure, IT System Availability, and Monitoring on MCS Awareness, and the subsequent influence of MCS Awareness on MCS Resiliency, with Fear of Cyber Attack as a moderating variable. The findings are expected to contribute to the development of more holistic and human-centered maritime cybersecurity strategies that strengthen cyber resilience at the operational shipboard level.

METHOD

This study adopts a quantitative research design using a structured questionnaire-based survey to examine the relationships between procedure availability (X1), IT system availability (X2), monitoring (X3), maritime cyber security awareness (Z), fear of cyber security (M), and maritime cyber security resiliency (Y). The target respondents are shipboard officers holding a valid Certificate of Endorsement (COE), as this certification is issued exclusively to officers and must be renewed every five years, ensuring that respondents represent actively sailing and professionally certified personnel. Based on administrative records, the population is estimated at 34,348 Indonesian officers, and the sample size was determined using the Slovin formula, resulting in 396 respondents, which was rounded to 400 respondents to improve statistical robustness. Primary data were collected through questionnaires using existing and validated indicators, while secondary data were obtained from relevant literature. Data analysis was conducted using Structural Equation Modeling - Partial Least Squares (SEM-PLS) with SmartPLS 4 to test direct effects, the mediating role of MCS Awareness, and the moderating role of Fear of Cyber Security in the proposed research model.

RESULTS AND DISCUSSION

Outer Model

1. Validity Testing

Table 1. Validity Testing

Variable	Indicator	*Loading Factor*	Description
Fear of Cyber Attack (M)	M1	0.852	VALID
	M2	0.873	
	M3	0.899	
	M4	0.927	
	M5	0.869	
	M6	0.905	
Procedure (X1)	X1.1	0.880	VALID
	X1.2	0.886	
	X1.3	0.846	
	X1.4	0.911	
	X1.5	0.868	
	X1.6	0.868	
IT System Availability (X2)	X2.1	0.844	VALID
	X2.2	0.888	
	X2.3	0.883	
	X2.4	0.917	
	X2.5	0.936	
	X2.6	0.923	

Monitoring (X3)	X3.1	0.888	VALID
	X3.2	0.880	
	X3.3	0.902	
	X3.4	0.931	
	X3.5	0.901	
	X3.6	0.913	
MCS Resiliency (Y)	Y1	0.885	VALID
	Y2	0.922	
	Y3	0.908	
	Y4	0.945	
	Y5	0.932	
	Y6	0.865	
MCS Awareness (Z)	Z1	0.869	VALID
	Z2	0.896	
	Z3	0.902	
	Z4	0.913	
	Z5	0.831	
	Z6	0.886	
Fear of Cyber Attack and MCS Awareness (M x Z)	MZ	1,000	VALID

Source: Research data

The convergent validity results indicate that all indicators across constructs demonstrate loading factor values well above the recommended threshold of 0.70, ranging from 0.831 to 0.945. This confirms that each indicator reliably represents its respective construct. Accordingly, all measurement items are considered valid and suitable for further analysis in both the measurement model and structural model.

2. Discriminant Validity

Table 2. Discriminant Validity Testing

	FOCA (M)	PROC (X1)	ITSA (X2)	MONT (X3)	MCSR (Y)	MCSA (Z)	FOCA x MCSA (M)
FOCA (M)							
PROC (X1)	0.566						
ITSA (X2)	0.679	0.675					
MONT (X3)	0.689	0.709	0.854				
MCSR (Y)	0.740	0.765	0.803	0.815			
MCSA (Z)	0.796	0.744	0.768	0.770	0.830		
FOCA x MCSA (M)	0.418	0.336	0.334	0.368	0.338	0.407	

Source: Research data

The discriminant validity assessment shows that the inter-construct correlation values range from 0.334 to 0.830, with the highest value remaining below the recommended threshold of 0.90. This indicates that each construct is empirically distinct and captures a unique conceptual domain. Therefore, the measurement model satisfies discriminant validity criteria and is appropriate for subsequent structural model evaluation.

3. Reliability Testing

Table 3. Reliability Testing

	Cronbach's alpha	Composite reliability (rho_c)
FOCA (M)	0.946	0.957
PROC (X1)	0.940	0.952
ITSA (X2)	0.952	0.962

MONT (X3)	0.955	0.964
MCSR (Y)	0.958	0.967
MCSA (Z)	0.943	0.955

Source: Research data

The reliability assessment shows that all constructs achieve Cronbach's alpha and composite reliability values well above the recommended threshold of 0.70, indicating a high level of internal consistency. These results confirm that the measurement items consistently measure their respective constructs and that the research instrument is reliable for further structural model analysis.

Inner Model

1. Coefficient of Determination

Table 4. Coefficient of Determination Testing

	R-square	R-square adjusted
MCSR (Y)	0.761	0.757
MCSA (Z)	0.648	0.645

Source: Research data

The coefficient of determination results show that MCS Resiliency (Y) has an R-square value of 0.761, indicating that 76.1% of the variance in MCS Resiliency is explained by its predictor variables, which reflects strong explanatory power, while MCS Awareness (Z) has an R-square value of 0.648, suggesting that 64.8% of its variance is accounted for by the exogenous constructs and can be categorized as moderate to substantial. The corresponding R-square adjusted values of 0.757 for MCS Resiliency and 0.645 for MCS Awareness remain very close to their respective R-square values, indicating stable explanatory capability after accounting for the number of predictors and confirming that the model does not suffer from overestimation. Overall, the consistency between R-square and adjusted R-square values demonstrates that the structural model exhibits good predictive accuracy.

2. F-Square Test

Table 5. f-square Testing

Variable	F-Square
Fear of Cyber Attack -> MCS Resiliency	0.051
Procedure -> MCS Resiliency	0.097
IT System Availability -> MCS Resiliency	0.044
Monitoring -> MCS Resiliency	0.049
MCS Awareness -> MCS Resiliency	0.054
Fear of Cyber Attack and MCS Awareness -> MCS Resiliency	0.005
Procedure -> MCS Awareness	0.167
IT System Availability -> MCS Awareness	0.085
Monitoring -> MCS Awareness	0.056

Source: Research data

The f-square results indicate that most relationships in the model exhibit small effect sizes, suggesting that each variable provides a modest but meaningful contribution to explaining MCS Resiliency and MCS Awareness. The strongest effect is observed in the relationship between Procedure and MCS Awareness, which approaches a moderate level and emphasizes the importance of clear and well-defined procedures in fostering cybersecurity awareness. The effects of Fear of Cyber Attack, IT System Availability, Monitoring, and MCS Awareness on MCS Resiliency are also categorized as small but relevant, while the interaction between Fear of Cyber Attack and MCS Awareness shows a very small additional contribution. Overall, although individual effects are relatively limited, the combined influence of all predictors enhances the explanatory strength of the structural model.

3. GOF

Table 6. GOF Testing

Variable	AVE	R-square adjusted
FOCA (M)	0.789	
PROC (X1)	0.768	
ITSA (X2)	0.809	
MONT (X3)	0.815	
MCSR (Y)	0.828	0.757
MCSA (Z)	0.780	0.645
Avarage	**0.798**	**0.701**

Source: Research data

The Goodness of Fit value of 0.748 indicates a large model fit, demonstrating that the proposed model has strong overall explanatory power and is capable of adequately representing the relationships among constructs. This confirms that both the measurement and structural models perform well and are suitable for hypothesis testing.

Hypothesis Testing

Table 7. Hypothesis Testing

	Original Sample	Standart Deviation	T Statistics	Pvalues (1 Tail)	Description
The influence of Procedure on Maritime Cyber Security (MCS) Resiliency	0.229	0.048	4,759	0.000	H1: Accepted
The influence of Procedure on Maritime Cyber Security (MCS) Awareness	0.335	0.060	5,620	0.000	H2: Accepted
The influence of IT System Availability on Maritime Cyber Security (MCS) Resiliency	0.190	0.071	2,665	0.008	H3: Accepted
The influence of IT System Availability on Maritime Cyber Security (MCS) Awareness	0.306	0.063	4,824	0.000	H4: Accepted
The influence of Monitoring on Maritime Cyber Security (MCS) Resiliency	0.208	0.068	3,038	0.002	H5 : Accepted
The influence of Monitoring on Maritime Cyber Security (MCS) Awareness	0.258	0.068	3,796	0.000	H6 : Accepted
The influence of Maritime Cyber Security (MCS) Awareness on Maritime Cyber Security (MCS) Resiliency	0.220	0.054	4,041	0.000	H7 : Accepted
The interaction effect of Fear of Cyber Attack and MCS Awareness on MCS Resiliency	0.026	0.020	1,307	0.191	H8: Rejected
IT System Availability influences MCS Resiliency through MCS Awareness	0.067	0.023	2,896	0.004	H9: Accepted
Monitoring influences MCS Resiliency through MCS Awareness	0.057	0.020	2,797	0.005	H10: Accepted
Procedure influences MCS Resiliency through MCS Awareness	0.074	0.022	3,369	0.001	H11: Accepted

Source: Research data

Discussions

The results (H1–H7) show that procedures, IT systems, and monitoring are key drivers of MCS Resiliency, both directly and through Maritime Cyber Security Awareness. The

significant positive effect of procedures on MCS Awareness and MCS Resiliency confirms that clearly documented, accessible, and consistently updated cyber procedures enhance seafarers' understanding of cyber risks and standardize secure operational behavior. This finding supports governance-oriented cybersecurity literature, which emphasizes that formalized policies and procedures translate abstract security requirements into actionable practices, thereby strengthening organizational preparedness and reducing human-related vulnerabilities (Troullinos, 2022). In maritime contexts characterized by highly interconnected IT/OT systems, procedural clarity becomes especially critical because it guides crew actions during abnormal cyber events and ensures continuity of operations.

The significant influence of IT System Availability on both MCS Awareness and MCS Resiliency further indicates that resilient and reliable onboard IT infrastructure forms the technological backbone of maritime cybersecurity. Systems that are well-maintained, redundant, and capable of rapid recovery from disruptions provide a stable environment in which security mechanisms can operate effectively. This result is consistent with research showing that robust IT/OT architectures increase situational awareness, enable timely detection of anomalies, and support faster recovery from cyber incidents (Waqas et al., 2021). Moreover, the positive relationship between IT System Availability and MCS Awareness suggests that continuous exposure to functional security features (e.g., authentication systems, access controls, and alerts) reinforces users' understanding of cybersecurity practices, thereby strengthening human–technology synergy in cyber defense.

Similarly, the acceptance of H5 and H6 confirms that monitoring capability is a crucial determinant of both awareness and resilience. Continuous monitoring, periodic risk assessments, and early warning systems enhance visibility over system status and emerging threats, which improves crews' situational awareness and responsiveness. This finding aligns with studies emphasizing that monitoring-based cybersecurity architectures, particularly those utilizing anomaly detection and correlation analysis, significantly improve early detection accuracy and threat comprehension (Vaarandi et al., 2025). In operational maritime environments, where system failures may directly affect navigation safety, effective monitoring becomes an indispensable component of resilience-building strategies.

The acceptance of H7 establishes MCS Awareness as a direct predictor of MCS Resiliency, indicating that awareness functions not merely as cognitive knowledge but as an operational capability that enables adaptive and protective behavior. Seafarers who understand cyber threats and appropriate countermeasures are more likely to comply with procedures, avoid risky digital practices, and respond effectively during incidents. This finding is consistent with empirical evidence showing that cybersecurity awareness enhances incident recognition, procedural adherence, and recovery performance, ultimately strengthening organizational cyber resilience (Netshiunda & Madzvamuse, 2025). Consequently, awareness acts as a central human-centered pillar in maritime cybersecurity.

In contrast, the rejection of H8 indicates that the interaction effect of Fear of Cyber Attack and MCS Awareness on MCS Resiliency is not statistically significant. This suggests that heightened fear or perceived threat alone does not strengthen the impact of awareness on resilience. This result supports prior studies which argue that fear-based responses may increase anxiety but do not necessarily translate into sustained protective behavior unless supported by adequate competence, training, and system capability (Sun et al., 2025). In high-risk operational domains such as maritime shipping, resilience appears to be driven more by structured preparedness and practical capability than by emotional threat appraisal.

Finally, the acceptance of H9, H10, and H11 confirms the mediating role of MCS Awareness in the relationships between procedures, IT system availability, monitoring, and MCS Resiliency. These findings indicate that organizational and technological investments do not automatically generate resilience; instead, their effectiveness depends on the extent to which they are internalized into seafarers' understanding and everyday operational behavior. This

interpretation is consistent with Netshiunda & Madzvamuse (2025) who emphasize that cybersecurity awareness bridges digital literacy, policy implementation, and technical infrastructure with tangible resilience outcomes. Thus, strengthening maritime cyber resilience requires an integrated approach that simultaneously enhances procedures, technology, monitoring, and human awareness rather than relying on isolated interventions.

CONCLUSION

This study provides empirical evidence that procedure availability, IT system availability, and monitoring capability are key determinants of Maritime Cyber Security (MCS) Resiliency, both directly and indirectly through Maritime Cyber Security Awareness. The findings confirm that clearly defined and consistently implemented cyber procedures, supported by resilient onboard IT systems and effective monitoring mechanisms, significantly enhance seafarers' awareness of cyber threats and appropriate protective actions. In turn, higher levels of MCS Awareness contribute substantially to stronger maritime cyber resilience, indicating that awareness functions as an operational capability rather than merely cognitive knowledge.

Furthermore, the study demonstrates that MCS Awareness serves as a central mediating mechanism that translates organizational and technological readiness into resilient cybersecurity outcomes. Organizational investments in procedures, infrastructure, and monitoring will not automatically yield resilience unless they are internalized into users' understanding and day-to-day operational behavior. Conversely, the non-significant moderating effect of Fear of Cyber Attack suggests that psychological threat perception alone is insufficient to strengthen resilience, underscoring that sustainable maritime cyber resilience is driven primarily by competence-based preparedness, structured governance, and system capability rather than fear-based motivation.

Overall, this research highlights the importance of adopting an integrated, human-centered, and system-oriented approach to maritime cybersecurity. Strengthening maritime cyber resilience requires simultaneous improvements in procedural governance, resilient IT infrastructure, continuous monitoring, and structured awareness-building among seafarers. These findings provide a robust empirical foundation for the development of more effective maritime cybersecurity strategies and competency frameworks, particularly in countries seeking to enhance the cyber readiness of their seafaring workforce.

REFERENCE

Afenyo, M., & Caesar, L. D. (2023). *Maritime cybersecurity threats: Gaps and directions for future research*. https://doi.org/10.1016/j.ocecoaman.2023.106493

Cook, P. (2020). Comment: The emerging spectrum of maritime security. *International Journal of Maritime Crime and Security*, *01*(01), 50–55. https://doi.org/10.24052/ijmcs/v01is01/art-5

Erstad, E., Ostnes, R., & Lund, M. S. (2021). An operational approach to maritime cyber resilience. *TransNav*, *15*(1), 27–34. https://doi.org/10.12716/1001.15.01.01

Heering, D., Maennel, O. M., & Venables, A. N. (2021). *Shortcomings in cybersecurity education for seafarers Shortcomings in cybersecurity education for seafarers*. *July*. https://doi.org/10.1201/9781003216582-6

Karas, A. (2023). Maritime Industry Cybersecurity: A Review of Contemporary Threats. *European Research Studies Journal*, *XXVI*(Issue 4), 921–930. https://doi.org/10.35808/ersj/3336

Netshiunda, H., & Madzvamuse, S. (2025). *A Systematic Literature Review of Cybersecurity Awareness and Strategy in Rural-Based Universities*.

Raymaker, A. (2024). A Sea of Cyber Threats : Maritime Cybersecurity from the Perspective of Mariners. In *Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security (CCS '25), October 13â•fi17, 2025, Taipei, Taiwan* (Vol. 1,

Issue 1). arXiv. https://doi.org/10.1145/3719027.3744816

Sun, M., Xu, S., Yuan, K., & Vortia, M. P. (2025). *Research on a Multidisciplinary Talent Development Model for High-End Shipping Services*. *2*(4), 1–13.

Troullinos, D. (2022). *Extending SUMO for Lane-Free Microscopic Simulation of Connected and Automated Vehicles*. 95–103.

Vaarandi, R., Tsiopoulos, L., Visky, G., Rehman, M. U., & Bahsi, H. (2025). A Systematic Literature Review of Cyber Security Monitoring in Maritime. *IEEE Access*. https://doi.org/10.1109/ACCESS.2025.3567385

Vaarandi, R., Tsiopoulos, L., Visky, G., & Rehman, M. U. R. (2025). *A Systematic Literature Review of Cyber Security Monitoring in Maritime*. *May*, 85307–85329. https://doi.org/10.1109/ACCESS.2025.3567385

Vrhovec, S., & Mihelič, A. (2021). Redefining threat appraisals of organizational insiders and exploring the moderating role of fear in cyberattack protection motivation. *Computers and Security*, *106*(April). https://doi.org/10.1016/j.cose.2021.102309

Waqas, M., Kumar, K., Ali, A., Saeed, U., Malook, M., Aftab, R., Shaikh, A., Hussain, F., Rai, A., & Qazi, A. Q. (2021). *Botnet attack detection in Internet of Things devices over cloud environment via machine learning*. *September 2019*, 1–23. https://doi.org/10.1002/cpe.6662

Yoo, Y., & Park, H.-S. (2021). *Qualitative Risk Assessment of Cybersecurity and Development of Vulnerability Enhancement Plans in Consideration of Digitalized Ship*.